

Controlled Link Sharing and Quality of Service Data Transfer for Military Internetworking

Joseph P. Macker
Center for High Assurance Computer Systems
Naval Research Laboratory
macker@itd.nrl.navy.mil

ABSTRACT

This paper discusses system design issues related to enhancing present internetworking architectures to achieve controlled link sharing and high assurance data interchange guarantees. The military services are implementing both wired and wireless Internet Protocol (IP) based data networks to provide interoperable, heterogeneous network connectivity. At present, internetwork routing products forward network data traffic with limited concern for the link sharing policies or the specific quality requirements of the traffic flow. An enhanced Integrated Services IP architecture is emerging which provides solutions for a rich set of resource sharing requirements. We present an overview of this architecture and discuss performance issues for candidate system components in a military context. The strong conclusion is that, based upon recent research and emerging technologies, a dynamic mixture of guaranteed services and controlled link sharing is achievable over operational packet networks. We recommend future work to validate candidate servicing models and to understand military application, security, and policy management requirements within this enhanced architecture.

1. INTRODUCTION

This paper discusses the need for *controlled link sharing* and *Quality of Service (QoS)* data transfer in future DoD internetworking architectures. The core theme of this paper is to discuss methods of improving military internetworking architectures to support *link sharing guarantees* and *high assurance networking services* for the information warrior. After establishing the rationale for QoS networking and link sharing, we will discuss the related performance issues and various system components required within an enhanced *integrated services packet network (ISPN)* architecture[18]. In addition, we discuss the use of related *open standard* traffic flow setup protocols, such as the *Resource ReSerVation Protocol (RSVP)* [3].

2. BACKGROUND

Perhaps the most innovative idea developed in data networking over the past 20 years has been the concept of *internetworking*. Internetworking technology hides many of the details of network hardware and permits data interchange

among computers regardless of the physical network connections. This innovation has been made possible through the development of internetworking protocols like the Internet Protocol (IP) and ISO's Connectionless Network Protocol (CLNP). The great success of this *open system* internetworking approach is evidenced by the recent exponential growth of the Internet and the widespread use and acceptance of distributed information services such as the World Wide Web (WWW).

The DoD is presently developing joint service multimedia applications, e.g., the Global Command and Control System (GCCS), and networking architectures, e.g., Army Task Force XXI, to interconnect global warfighting entities and improve both interoperability and mission performance. A large portion of this infrastructure is planning to adopt "de facto" standard Internet Protocol (IP) based internetworking technology. Military communication often requires operation over low to medium bandwidth wireless links and will likely require that multiple communication system users or groups be provided a minimum service quality to sustain priority communications through congestion conditions. It is therefore important to understand the QoS and link sharing limitations of current IP technology.

At the core of the DARPA TCP/IP protocol suite is the IP protocol. IP is a datagram-oriented protocol providing *best effort* delivery between end systems attached to an IP internetwork [2]. *Best effort* implies that IP packets are treated as if all are equally important, and while IP makes an effort to deliver all packets to their destination, packets may occasionally be delayed, lost, duplicated, or delivered out of order.

As more battlefield systems migrate to internetworking concepts, contention for shared communication resources will increase. A present feature of IP routers is that as offered traffic load increases each communication flow receives less of the overall capacity and is increasingly delayed in a nondeterministic manner. This effect can be exacerbated over low-to-moderate bandwidth wireless network links, as those typically used between warfighting units. Therefore, to satisfy future military internetwork needs, a mechanism is required to effectively resolve and service competing data flow requirements, including support for both

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 1996		2. REPORT TYPE		3. DATES COVERED 00-00-1996 to 00-00-1996	
4. TITLE AND SUBTITLE Controlled Link Sharing and Quality of Service Data Transfer for military Internetworking			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Research Laboratory,Center for High Assurance Computer Systems,4555 Overlook Avenue, SW,Washington,DC,20375			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 8	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

*flow*¹ guarantees and hierarchical link sharing. An enhanced ISPN architecture can provide this mechanism.

provide a unified approach to extending *IS* concepts to an internetwork architecture [21].

3. EVOLVING TECHNOLOGIES

Some of the detailed technical requirements necessary to provide a mixture of flow guarantees in an ISPN architecture are still the subject of debate and continued research. However, there appears to be general agreement within the IP research community on a basic architectural framework [21] and numerous proposals, software implementations, simulation studies, and theoretical findings are emerging. The probability of widespread commercial transition of ISPN technology appears favorable as the Internet Engineering Task Force (IETF) and other technical standards bodies (e.g., ATM Forum) are actively pursuing protocols and standards for supporting QoS based networking. In addition, numerous commercial networking vendors are planning product releases in the near future. Within the limited space available, this paper discusses key performance issues, protocols, and components involved in providing service enhancements to a heterogeneous internetworking architecture.

3.1 INTEGRATED SERVICES INTERNETWORKING COMPONENTS

Supporting multiple traffic quality levels and effective link sharing guarantees over an internetwork requires an enhanced architecture, and the term *integrated services (IS)* model is often used to refer to an enhanced Internet service model including *best-effort*, *real-time*, and *controlled link sharing services* [18]. There are two basic core components to this new architecture.

- Traffic control: *what support is provided for classifying, admitting, and forwarding packets?*
- Reservation setup and maintenance: *how is service specified and established?*

The traffic control segment of this model includes three components: the packet scheduler, the classifier, and admission control [21]. The following sections provide some background and discussion of these technology components within the enhanced architecture. QoS-capable routing algorithms (e.g., M-OSPF [9]), while recognized as another important component available for achieving overall end-to-end service enhancements, will not be discussed in this paper. The architecture elements, protocols, and interfaces discussed here

3.2 PERFORMANCE GUARANTEE MODELS

What is a networking application generally interested in guaranteeing? Typical service features of are loss rate, bandwidth, and delay characteristics. Here we discuss the servicing mechanism which attempts to achieve guarantees and is part of the traffic control component of the *IS* extension model.

The packet forwarding mechanisms designed to provide a service guarantee can be broadly classified as providing *deterministic* or *statistical* guarantees, or in some cases both. The type of guarantee offered affects both complexity and overall performance.

It is assumed here that enhanced internetwork routers will implement improved queue management schemes for data flow management. It is in the queue management scheme that packet scheduling takes place. The scheme must be tightly coupled to the link layer protocol for the output media. The packet scheduler must invoke the appropriate link layer controls when the underlying media has a particular bandwidth allocation mechanism. For point-to-point interfaces, network layer queueing guarantees translate directly. However, translating the guarantees between the IP kernel queue and the link technology becomes more complex within non-overprovisioned broadcast network interfaces, and becomes particularly troublesome for multiple access wireless networks.

Internetworking routers essentially use the concept of *statistical multiplexing* in performing their function. The strong law of large numbers is often used as the rationale behind all statistical multiplexing approaches. This says that for a large number of uncorrelated flows, the total bandwidth required to satisfy all flows stays nearly constant. For this result to hold strictly, the flows must be statistically uncorrelated. If the law of large numbers holds, it is possible for mixed guaranteed and nonguaranteed services to be supported. While the guarantees provided by this form of multiplexing are only statistical and not deterministic, they can be made quite good for scenarios in which network behavior is well understood [20]. The problem with this model is the assumption that nonguaranteed traffic is random and uncorrelated and therefore can be predicted as an aggregate steady flow which will not significantly interfere with a simultaneous guaranteed service. Contrary to this assumption, recent studies and research have shown that network data traffic is often not random and therefore does not aggregate according to the strong law of large numbers. Rather, network data has been shown to be *fractal* in nature or *self-similar* [13]. Thus, a key assumption required for statistical multiplexing to work effectively may be absent from many actual networks. One way around the preceding traffic correlation problem is by *massaging* the traffic in the network to appear more random by

¹ *Flow* is a term used throughout this paper to refer to a delivery graph from a sender to one or more receivers [22]. While a network application's flow may contain a mixture of QoS requirements, we refer to a flow guarantee as the part of the flow requiring a specific QoS.

implementing traffic mixing within the network or applying traffic shaping approaches. In spite of its limitations *statistical multiplexing*, remains the simplest of all queue management approaches and can be important where simplicity is the primary concern.

Weighted fair queueing (WFQ) is a queue management approach designed to provide more deterministic flow guarantees than those provided by statistical multiplexing. Fair queueing requires the routers to maintain a separate queue for each flow and, when a source misbehaves causing congestion, only its queue is affected by the congestion. WFQ can provide strong guarantees to a set of traffic flows, and given that certain assumptions are satisfied, there is a well known result from Parekh [23] that the worst case delay bound for flow_i is

$$D_i = \frac{\beta_i}{\text{resrate}_i} + \frac{(\text{hops}_i - 1)\text{len}_{\max \text{flow}_i}}{\text{resrate}_i} + \sum_{m=1}^{h_i} \frac{\text{len}_{\max \text{net}}}{\text{linkrate}_m} \quad (1).$$

where,

- β_i = token bucket depth for flow i
- resrate_i = reserved rate for flow i
- hops_i = number of hops for flow i
- $\text{len}_{\max \text{flow}_i}$ = maximum packet size for flow i
- $\text{len}_{\max \text{net}}$ = maximum packet size for the network
- linkrate_m = network interface rate for link m

Equation (1) is an important result since it can be used to examine the upper bound performance features and requirements for weighted fair queueing given a particular network and flow scenario. The equation can be inverted to solve for a number of interesting parameters given a flow requirement, e.g., reservation bandwidth given a fixed latency bound. In Section 4, we will examine some example scenarios of WFQ performance bounds for a fictitious moderate rate military wireless network link.

WFQ provides a means to guarantee that a data flow receives a particular share of the network bandwidth while meeting a firm delay bound. In order to achieve deterministic guarantees for a given flow the worst case delay bounds can be large. Considering military wireless networks supporting low to moderate rate interface speeds, the added complexity of WFQ in the router appears to be a reasonable tradeoff for obtaining deterministic performance guarantees. Also, router products presently exist which implement WFQ schemes.

In order to improve upon the worst case delay performance of WFQ and provide a richer class of service guarantees, work has been done by Clark, Shenker, and Zhang (CSZ) to compromise between the simplicity of statistical multiplexing and the complexity and absolute guarantees of deterministic schemes [18]. Basically, the problem with strict first-in first-out (FIFO) queueing approaches for statistical multiplexing is that worst case performance occurs when packets find themselves behind bursts of traffic from other flows at intermediate hops. Over a number of hops, this can result in a large worst case delay. To combat this problem,

CSZ groups flows into classes and dynamically tracks the average queueing delay of each class at each hop. A flow's scheduling precedence within the queue at each hop is determined by whether it is ahead or behind its average delay performance estimate. While capable of performing some guaranteed service (e.g., WFQ at the higher classes), the focus of the CSZ approach is on the satisfaction of *predictive* service guarantees and away from extensive isolation of flows. *Predictive* service is guaranteed based upon the router's present understanding of network behavior, which may change dramatically over time. It is the basic goal of *predictive* service to satisfy a set of more tolerant, adaptive applications than those requiring strict absolute performance bounds.

Related work has been done by Floyd, Jacobson, et al to implement a Class Based Queueing (CBQ) design [5]. The concept developed here starts with the notion of controlled link sharing between multiple organizations or agencies allowing minimum bandwidth guarantees to each agency when required. A representation of a controlled link sharing scenario is shown Figure 1. The communication link or resource at the top of the tree represents 100% of the available bandwidth to share. This total bandwidth is divided amongst groups 1-3 and each group is provided a minimum bandwidth allocation guarantee. The final tier on the tree represents individual data flows and each is allocated a minimum percentage of the group's bandwidth.

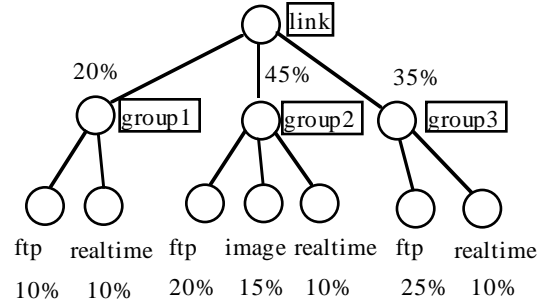


Figure 1: CBQ hierarchical link sharing

When bandwidth is not in use by a particular agency or flow, other services can use it. The borrowing and recovery of bandwidth from other flows is governed by the hierarchical arrangement of allocations and the location of overdrawn flows. This provides a novel means for implementing a sharing policy directly within the packet forwarding scheme itself. The CBQ model can be adapted to also provide allocations for real-time traffic flows by guaranteeing bandwidth and low delay for designated *priority-1* services. The implementation of CBQ unifies a number of essential elements required in future traffic controller designs: packet classifier, packet scheduler, and queue manager.

A form of a CBQ filter has been used to improve traffic management across the Trans-Atlantic link (FAT pipe) connecting various internetworking entities: the UK MoD and

the US DoD, European Space agency (ESA) and NASA, and the UK academic IP network and the US academic network [8]. This has allowed a movement away from “hard” sharing approaches (i.e., fixed multiplexing) to more economical “soft” sharing approaches. Each agency is guaranteed a fixed percentage as a minimum bandwidth for mission operation and unused bandwidth within these percentages is reallocated dynamically to handle any excess traffic.

In summary, a number of packet classification and forwarding approaches exist that, when combined with other networking components, e.g., traffic shaping assumption, can provide performance guarantees to data traffic flows. Additional techniques were not discussed due to space limitation (e.g., Jitter-EDD [29]). The ability to guarantee worst case deterministic performance in the face of internetwork congestion conditions (e.g., WFQ) seems to be an appropriate match for mission critical situational data flow in a future Military Internet, but extensive application of this approach has limitations in terms of overall admission control and worst case delay. There is most likely a mixture of best effort, predictive, and guaranteed data flow requirements among and within future military applications. A hybrid approach is a good long term goal for future military internetworks. The CBQ concept with its emphasis on multiple queue class hierarchy matches well with anticipated controlled link sharing requirements. While providing high assurance networking services to designated data flows, it also integrates policy-based sharing associated with interconnecting agencies or mission area components across common resources. There are a number of performance tradeoffs for the various approaches and simulation and demonstration of performance under a variety of military networking scenarios and traffic flow models is recommended. This work will predict performance bounds for desired application service guarantees and allow for further architecting of flow policies and appropriate resource management strategies.

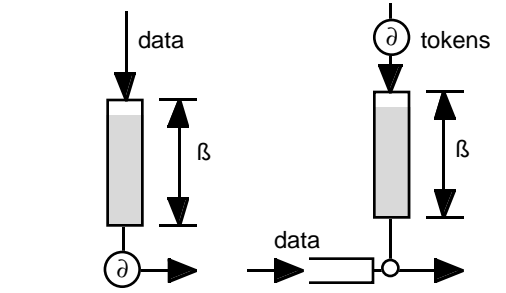
3.3 TRAFFIC SHAPING

An accurate description of a flow’s traffic patterns can, in many cases, help a network better manage its resources. Traffic shaping is a means for a particular data flow to describe its traffic characteristics to the underlying network. By understanding a flow’s characteristics the network can choose to reject a flow (admission control) and the network can monitor existing flows to check their behavior. We will briefly discuss a few simple traffic shaping approaches below.

The simplest form of traffic shaping is *isochronous* which attempts to shape traffic into a flow of packets spaced at equal time intervals [10]. The simple leaky bucket, see Figure 2(a), is modeled as a bucket with depth β and output rate ∂ . The data source places data to be sent into the bucket and data is drained out at the rate ∂ . The depth β determines how much data can be buffered prior to being sent over the

network. If data insertion exceeds the bucket depth, the data is discarded. The network is assured that the source will never inject data faster than ∂ into the network and maximum delay for data to enter the network is bounded by β .

The major advantage to the simple leaky bucket traffic shaping approach is its ease of implementation. Its downfall is its limitation describing the behavior of a traffic flow. Long term variable rate flows must request their peak rate of flow from the leaky bucket. This can be quite wasteful in terms of bandwidth allocation and admission control.



(a) Simple Leaky Bucket (b) Token Bucket

Figure 2: Traffic Shaping Models

While isochronous traffic shaping can be simple and useful, there exist more sophisticated means for shaping more complex traffic patterns. Describing traffic patterns more effectively translates to an ability for the network to allocate resources more effectively. The token bucket, see Figure 2(b), is a simple example of a more capable traffic shaping model. The token bucket modifies the leaky bucket model by using the bucket portion to regulate flow rather than buffering the actual traffic. The rate ∂ is the rate at which tokens are placed in the bucket and the bucket token depth is β as before. To transmit a packet, a number of tokens representing the size of the packets must first be removed by the traffic regulator from the bucket. The token bucket model provides a richer set of potential traffic patterns over a given time interval than the leaky bucket model. Additional output rate controls can be added to the token bucket model to limit its worst case maximum transmission rate performance to create a more well-behaved short term output [20].

We have briefly presented traffic shaping models, because they can contribute to the successful execution of network guarantees by providing a means to control and successfully describe a diverse set of user data flows. We will next discuss the setup of services for traffic flows within an ISPN.

3.4 TRAFFIC FLOW SETUP

How does an application or middleware entity ask for a specific flow and how does the network respond?

3.4.1 Flow Specification

In order to establish any special services for a flow, an application should be able to communicate the requirements of the flow to any servicing entities. This description of a flow's requirements is called a flow specification or *flowspec*. There are a number of application requirements which may be important to convey in a flow spec, such as delay and bandwidth, packet loss sensitivity, and traffic shaping description. There is some disagreement on how these descriptions should be conveyed to the network, by macro class definitions or by specific parameter lists. An example of a parameter list for a flowspec comes from RFC 1363 [22] and is shown below in Figure 3.

bit 0	7	15	23	31
Version		Maximum Transmission Unit		
Token Bucket Rate		Token Bucket Size		
Max. Transmission Rate		Minimum Delay Noticed		
Maximum Delay Variation		Loss Sensitivity		
Burst Loss Sensitivity		Loss interval		
Quality of Guarantee				

Figure 3: Flow Spec Example

3.4.2 Flow Setup Protocols

Note that the setup protocol component of the *IS* model does not provide any flow guarantee, but is used to provide information to the network about resource requirements and to negotiate appropriate QoS values for meeting the end-to-end system application requirements. We concentrate here on those setup protocols designed for an internetworking environment. Two such protocols, ST-II and RSVP, are the most interesting for consideration within the military environment

3.4.2.1 ST-II

ST-II is a revised version of the original Internet Stream Protocol (ST) [12]. ST-II was originally developed in 1990 to support transmission of real-time simulation data [11]. The approach of ST-II is to provide an integrated solution to flow setup by combining data transmission and resource reservation. This integrated approach allows QoS routing and resource availability to be made more easily. ST-II establishes reservations by transmitting a flow specification from the source to all receivers. Intermediate routers may adjust the flow specification based on locally available resources prior to the specification being transmitted back to the source. Thus, ST-II is sender-oriented and each source has knowledge of its receivers.

3.4.2.2 RSVP

RSVP is being designed to provide a number of capabilities [17]:

- Support multicast and unicast data distribution with possibly changing membership and routes.
- Provide transparent operation through routers not supporting RSVP.
- Provide multiple reservation models to fit a variety of applications.
- Treat reservation parameters as “opaque data” so that a variety of traffic control modules/techniques can be used to interpret and enforce them in different parts of a heterogeneous network.

RSVP control messages will be transported throughout the network as IP datagrams. “RSVP-aware” nodes (i.e. routers or hosts with RSVP functionality) will intercept RSVP messages and process them accordingly. Figure 4 illustrates the basic rsvp host to router interaction and also shows that each distributed rsvp process interfaces directly to a local traffic control module responsible for executing the packet classification and forwarding process.

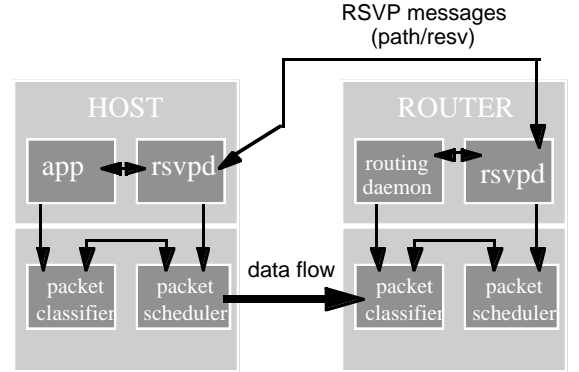


Figure 4: RSVP Host - Router Interaction

Two primary RSVP message types distribute resource reservation requests throughout the network: the *Path* message and the *Resv* message types. These messages are used to establish and maintain a simplex reservation from a sender to a receiver. A basic RSVP reservation proceeds as follows. After initialization, an RSVP capable source begins transmitting *Path* messages periodically. These messages inform RSVP nodes along the data path of the potential for a receiver to request a reservation along that data path. There is a timeout associated with these messages which can be adapted and as routing of data changes, the periodic *Path* messages will follow routing changes. In a network with QoS-based routing, it will be desirable that *Path* messages for a particular data source follow routing metrics that the sender anticipates will be useful for attaining the desired QoS data delivery for that data source. RSVP nodes respond to Path messages by storing

state information (e.g., incoming interface, previous RSVP node) and then forwarding the *Path* message on towards the receiver.

When the receiver wishes to request a reservation for a *Path* message received, the receiver generates a *Resv* message in the reverse direction of the *Path* messages received for that identifier. The specification (flowspec) for the receiver's desired QoS is attached to these messages, and each RSVP node along the reverse path processes, accepts or rejects (notifies receiver of rejection) the request, and then forwards the request for reservation on a hop by hop basis back to the sender. In the multicast case, these flowspecs may be merged with other group flowspecs upstream towards the source. As with the *Path* messages, reservations can time out; consequently, a robust "soft state" is maintained by periodically repeating *Resv* messages. Reservations can be updated and altered by changing the flowspec attached to the *Resv* messages.

4. ARCHITECTURAL ISSUES AND EXAMPLES

A number of architectural issues and engineering performance tradeoffs arise when implementing the *IS* enhancements to an existing packet network infrastructure. Some of the most vexing questions facing the public and commercial Internet's future relate to the establishment and enforcement of distributed behavioral policies within this more capable internetwork architecture. Perhaps one advantage of the DoD community is the potential for a more unified agreement and enforcement of homogeneous policies relating to controlled link sharing and high assurance traffic flow since there is likely more direct ownership and control over much of our own infrastructure.

4.1 GUARANTEED SERVICE EXAMPLES

This section examines in more detail the potential performance issues associated with providing guarantees within an *IS* internetwork architecture. We will examine the issues relating to the application of WFQ as a packet scheduling component by using equation (1) from Parekh.

4.1.1 Latency Bounds for Guaranteed Bandwidth

Given a fixed bandwidth reservation, what is the latency performance bound for a given network servicing model? In general, the differences in performance become more pronounced as the number of traversed hops increases. We present a set of simplified examples based upon the worst case performance bounds of WFQ.

The example scenario uses the following example parameters for the service, which may be characteristic of a

low-to-moderate rate wireless network carrying a situational awareness data flow:

- link rate for each hop = 64 kbps
- reasonable MTU for each link = 576 bytes
- Max app packet size = 100 bytes
- token bucket size = 1000

First, we reserve a number of fixed bandwidths and are interested in determining the upper bound delay characteristics for these guarantees to be satisfied. The results are shown in Figure 5.

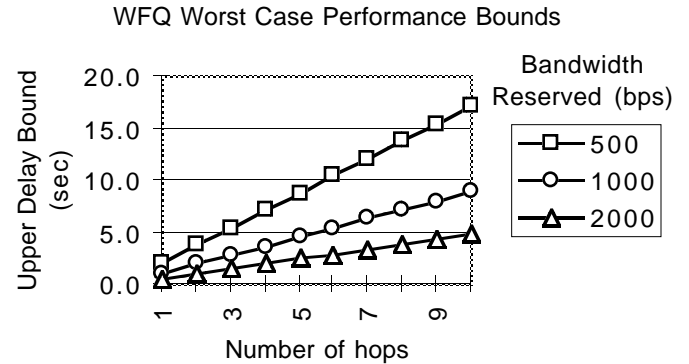


Figure 5: WFQ latency bounds

Figure 5 demonstrates the effect of increasing hop count and reserved bandwidth on the upper delay bound for a flow. This is a simple example the results represent the satisfaction of a worst case performance bound. Typical average performance would likely be somewhere below this bound. However, for a military networking environment, it is prudent to design with the worst case scenario in mind and these types of curves give us a clue as to the performance requirements for guaranteed service.

4.1.2 Required Minimum Reserved Bandwidth for Guaranteed Latency

The following example looks at WFQ from a different angle. Given a fixed delay requirement for a flow, what is the required bandwidth reservation to meet that guarantee? The answer affects admission control performance and is somewhat synonymous with the previous section. Once again, the differences in performance become more significant as the number of traversed hops increases.

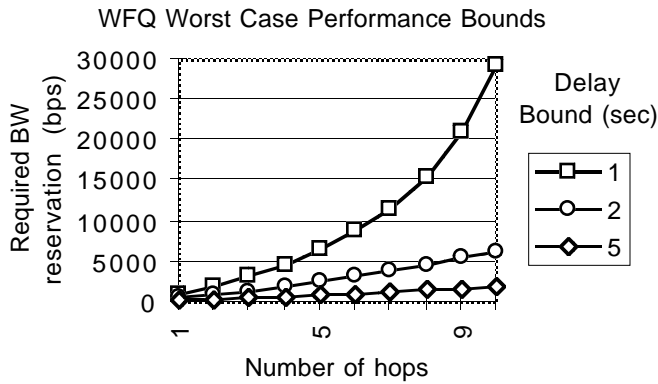


Figure 6: WFQ required bandwidth for latency bound

As an alternative to deterministic guaranteed service, it has been the claim of probabilistic techniques that good average latency design goals can be achieved with less complexity than required by WFQ and related approaches. This is a potential risky proposition for the military environment, owing to the unpredictable worst case behavior, but the potential performance tradeoffs warrant further study. Certainly probabilistic techniques are a good design approach for predictive service requirements.

4.2 SECURITY AND POLICY ISSUES

New network security issues are raised by providing an additional capability of resource reservation in routers. Once this enhanced architecture is in place, certain users of the network are granted privileged services and this implies a need for improved policy and administrative controls. Network authentication of traffic becomes more critical. There are several types of authentication required: authentication of users requesting services, authentication of the packets using a service, and authentication of packets modifying policy in routers.

RSVP is a protocol for establishing distributed state in routers and hosts and allows the endpoints to reserve resources within an *IS* networking infrastructure. Permission for a reservation will depend upon resource availability and policy satisfaction. Unlike end-to-end security techniques, RSVP control messages require hop-by-hop security features. RSVP cryptographic authentication has been proposed [18]. The technique is independent of the cryptographic algorithm is presently planned to use an MD5 message digest. A side benefit of the authentication is that it also results in improved message integrity. This solution provides authentication for service requests and control. Authentication approaches for packets using a service are presently being discussed. The application of standard IP security (IPSEC) formats is likely [24,25,26,28].

The distributed management of link sharing policies (e.g., placing of link sharing hierarchy rules in routers)

requires a strong security approach. Allowing uncontrolled access to such a major resource management function would be unwise. Initially such policies can be statically configured in the routers, but a better long term solution would be to establish a link sharing policy management information base (MIB) and use a distributed, secure network management approach (e.g., secure SNMP). Such an approach better supports the changing resource requirements at different stages of a battle.

5. SUMMARY

QoS based data transfer and controlled link sharing will provide needed capability for robust, dynamic management of shared resources among the many applications and user communities being integrated within DoD networks. Those involved in the development of future military internetworking and applications should move to better understand and integrate this emerging technology. With a better grasp of future integrated networking requirements DoD will be in a better position to influence standards development and verify service model performance. The diversity of unique DoD communications and application requirements (e.g., multimedia data distribution, teleconferencing, distributed mission planning, situational awareness data flow, wireless mobile networking, distributed interactive simulation) make this investment necessary.

6. REFERENCES

- [1] Zhang, L., "Designing a New Architecture for Packet Switching Communication Networks", IEEE Communications Magazine, Sept. 1987.
- [2] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", Proceedings of the ACM SIGCOMM '88, August 1988.
- [3] Zhang, L., S. Deering, D. Estrin, S. Shenker, and D. Zappala, "RSVP: A New Resource Reservation Protocol," IEEE Networks Magazine, September 1993.
- [4] Stevens, W.R., TCP/IP Illustrated, Volume 1. Addison-Wesley Publishing Company, Reading, Massachusetts, 1994.
- [5] Floyd, S., "Link-Sharing and Resource Management Models for Packet Networks", Technical report, Lawrence Berkeley Laboratory, December 14, 1994.
- [6] Althouse E.L., J.P. Macker, J.P. Hauser, and D.J. Baker, "Integrated Services in Tactical Communication Systems," 1995 NRL Review, pp. 141-143.
- [7] Deering, S. "Host Extensions for IP Multicasting". Internet RFC 1112, August 1989.
- [8] Wakeman I, A. Ghosh, J. Crowcroft, V. Jacobson, and S. Floyd, "Implementing Real Time Packet Forwarding Policies

using Streams", Usenix 1995 Technical Conference, January 1995.

[9] Moy J., "Multicast Extension to OSPF". Internet Draft, September 1992.

[10] Turner, J.S., "New Directions in Communications (or Which Way to the Information Age)," IEEE Communications, Vol.24, No.19, October 1986, pp 8-15.

[11] Topolcic C., S. Pink, " An Implementation of the Revised Internet Stream Protocol (ST-2)," Journal of Internetworking: Research and Experience, vol.3 no.1, March 1992.

[12] Forgie, J., "ST- A Proposed Internet Stream Protocol," Internet Experimental Notes IEN-119, September 1979.

[13] Leland, W.E.,M.S. Taqqu, W. Willinger, and D.V. Wilson, "On the Self Similar Nature of Ethernet Traffic." Proc. ACM SIGCOMM '93, September 1993.

[14] Jacobson, V.,. "A Portable, Public Domain Network Whiteboard", April 1992. Xerox PARC, viewgraphs.

[15] Jacobson, V., "Multimedia Conferencing on the Internet", August 1994. Tutorial 4, ACM SIGCOMM 94.

[16] McCanne S., "A Distributed Whiteboard for Network Conferencing", May 1992. UC Berkeley CS 268 Computer Networks term project.

[17] Braden, R., L. Zhang, S. Berson, Z. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Funtional Specification", Internet Draft (work in progress), February, 1996.

[18] Clark, D., S. Shenker, and L. Zhang. "Supporting Real-time Applications in an Integrated Services Packet Network: Architecture and Mechanism". In Proc. ACM SIGCOMM, September 1992.

[19] Postel J., "Transmission Control Protocol - DARPA Internet Protocol Program Specification". Internet RFC 793, September 1981.

[20] Partridge C., "Gigabit Networking". Addison-Wesley Professional Computing Series, 1994.

[21] Braden B., D. Clark, and S. Shenker," Integrated Services in the Internet Architecture: an Overview". Internet RFC 1633, June 1994.

[22] Partridge C., "A Proposed Flow Specification", RFC-1363, July 1992.

[23] Parekh, A., "A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks", Technical Report LID-TR-2089, Laboratory for Information and Decision Systems, MIT, 1992.

[24] Atkinson, R. , "Security Architecture for the Internet Protocol", RFC 1825, NRL, August 1995.

[25] Atkinson, R. , " IP Authentication Header", RFC 1826, NRL, August 1995.

[26] Atkinson, R. , " IP Encapsulating Security Payload", RFC 1827, NRL, August 1995.

[27] Baker, F., "RSVP Cryptographic Authentication", Internet Draft, work in progress, November 1995.

[28] Berger, L., T. O'Malley, R. Atkinson, "Proposed RSVP Extensions for IPSEC IPv4 Data Flows", Internet Draft, work in progress, February, 1996.